SOBERANÍA, RESISTENCIA Y AUTODEFENSA ELECTRÓNICA EN TELÉFONOS MÓVILES:

PARTE 1

VIGILANCIA MASIVA | PERFILAMIENTO Y METADATOS | AMENAZAS EN REDES MÓVILES | PRIVACIDAD Y CIFRADO | RESISTENCIA Y SOBERANÍA | SOFTWARE LIBRE Y COMUNIDAD

RECUPERA EL CONTROL. PROTEGE TU PRIVACIDAD. DEFIENDE TU LIBERTAD.

USO Y FUNCIONAMIENTO

- Cómo usamos nuestros teléfonos
- Sensores, conexiones y tecnología interna

AMENAZAS Y VIGILANCIA

- Stingrays, SIM jacker, SS7, Cell Tower Dump
- Telemetría, perfiles, metadatos y vigilancia masiva

SISTEMAS ALTERNATIVOS

- Sistemas móviles libres, seguros y respetussos de tu privacidad
- Control total de tu dispositivo

TIENDAS DE APLICACIONES

- Tiendas libres y seguras
- Alternativas a Google Play Store

DESGOOGLEA TU TELÉFONO

- Herramientas para liberarte de Google
- Beneficios, procesos y riesgos

PRIVACIDAD ES PODER • CONOCIMIENTO ES DEFENSA • UNIDAD ES FUERZA

CYPHERPUNK • PRIVACY • FREEDOM • OPEN SOURCE • RESISTANCE

Los teléfonos móviles se han convertido en extensiones omnipresentes de nuestra vida cotidiana. Además de servir como herramientas de comunicación y entretenimiento, estos dispositivos gestionan información personal, realizan transacciones financieras, registran nuestra ubicación y estimulan nuestras emociones. Su ubicuidad plantea un desafío crítico: ¿hasta qué punto somos conscientes de la dependencia que hemos creado respecto a ellos y de cómo nuestros datos son aprovechados? En la era de la economía de la atención, las aplicaciones y servicios buscan captar y retener nuestra mirada constantemente, fomentando patrones de uso adictivos para obtener rentabilidad a partir de nuestros datos. Esto erosiona nuestra privacidad y puede condicionar comportamientos sin que lo notemos.

Por otro lado, la sofisticación técnica de los smartphones los convierte en nodos de vigilancia masiva. Cada componente –desde la cámara y el micrófono hasta el GPS y el acelerómetro– no solo habilita funciones útiles, sino que también puede servir para monitorizar al usuario y su entorno. Las infraestructuras de red móvil están sujetas a amenazas de intercepción y manipulación, y las compañías tecnológicas acumulan ingentes cantidades de metadatos sobre nuestros hábitos. En este contexto, surge la necesidad de hablar de soberanía digital, resistencia y autodefensa electrónica: es decir, de tomar medidas conscientes para proteger nuestros datos, limitar la intrusión en nuestra vida privada y elegir herramientas que refuercen el control individual sobre el teléfono.

En esta guía extensa se analiza primero cómo usamos y cómo funcionan nuestros teléfonos móviles, para luego exponer las amenazas de vigilancia y perfilamiento que enfrentamos. Después se presentan alternativas tecnológicas: sistemas operativos libres y seguros, tiendas de aplicaciones alternativas y herramientas para “desgooglear” el dispositivo. Finalmente, se ofrecen conclusiones y recomendaciones prácticas orientadas a la autodefensa electrónica y la soberanía digital.

1. Uso y funcionamiento de los teléfonos móviles

Los teléfonos inteligentes son dispositivos multifunción que nos acompañan prácticamente a cada momento. Para comprender la soberanía digital, es fundamental analizar **cómo los usamos** y **cómo operan** en su interior. De este modo podemos visualizar no solo las comodidades que ofrecen, sino también los riesgos implícitos en nuestra relación con ellos.

¿Cómo usamos nuestros teléfonos?

El uso de los smartphones trasciende la simple comunicación. Habitualmente llevamos encendido el dispositivo todo el día: lo consultamos nada más despertar y por última vez antes de dormir. Usamos redes sociales para interactuar, aplicaciones de mensajería para hablar con amigos y familiares, navegamos por Internet, escuchamos música, vemos videos y realizamos pagos o gestión bancaria. Esta multiplicidad de actividades hace que el teléfono acumule inmensas cantidades de información personal, desde contactos y horarios hasta gustos y movimientos.

Pero además de centralizar funciones, los teléfonos inteligentes están diseñados para capturar nuestra **atención**. Las aplicaciones utilizan notificaciones, diseños psicológicamente estudiados, actualizaciones constantes y recompensas intermitentes (por ejemplo, el sistema de “likes” en redes sociales) para generar hábitos de uso frecuentes y prolongados. Este fenómeno se inscribe en la llamada *economía de la atención*, donde las empresas compiten por retener el tiempo y la energía mental del usuario. Dado que los anunciantes monetizan este ecosistema (vendiendo espacios publicitarios y datos de los usuarios), existe un incentivo directo en que las aplicaciones nos enganchen.

Como resultado, se observa una dependencia creciente: muchas personas sienten incomodidad o ansiedad cuando no tienen su teléfono cerca, revisan compulsivamente las pantallas cada pocos minutos, o utilizan el dispositivo mientras realizan otras tareas (“multitasking” constante). Este patrón de **adicción tecnológica** afecta la calidad del sueño, la concentración y las relaciones personales. Además, al pasar tanto tiempo conectados, generamos un rastro digital continuo: nuestros hábitos de navegación, posición geográfica, consumo de contenidos e incluso nuestras pulsaciones en teclado son recopilados. Entender este aspecto nos permite ser más críticos con el uso que hacemos del teléfono y empezar a tomar decisiones que reduzcan la intrusión en nuestra vida privada.

Adicción, dependencia y economía de la atención

El término “economía de la atención” describe cómo diferentes servicios digitales compiten por un recurso escaso: nuestra concentración. Cada notificación emergente, cada “sonido de alerta” o cada actualización visual está calibrado para interrumpir nuestra actividad y hacernos volver a la aplicación. De este modo, pasamos más tiempo en esas plataformas: más clics, más datos registrados, más ingresos por publicidad. Desde una perspectiva de soberanía digital, este

diseño adictivo es problemático porque nuestro comportamiento y decisiones se transforman en producto comercializable. Los algoritmos analizan qué nos mantiene enganchados para inducir conductas aún más dependientes.

Para mitigar estos efectos, es importante desarrollar una relación crítica con el teléfono: establecer límites de uso consciente, desactivar notificaciones no esenciales, y recurrir a aplicaciones que ayuden a medir o restringir el tiempo de pantalla. También podemos reflexionar sobre las intenciones de cada aplicación: cuestionar si necesitamos ese servicio o si hay alternativas más saludables (por ejemplo, usar un calendario local en lugar de una app social, o escuchar música descargada en lugar de streaming). Al recuperar cierto control en el uso diario del móvil, damos un primer paso hacia la **resistencia digital** frente a la explotación de nuestra atención.

¿Cómo funcionan nuestros teléfonos?

Técnicamente, un teléfono móvil moderno es una computadora de bolsillo, equipada con una gran variedad de **sensores** y **módulos de comunicación**. Cada componente contribuye a funciones concretas: tomar fotos, ubicarnos en mapas, reconocer nuestros gestos o incluso medir parámetros ambientales. Al mismo tiempo, casi todos estos subsistemas pueden ser utilizados para rastrearnos. A continuación se describen los más relevantes:

- **Pantalla**: Es la interfaz principal con el usuario. Las pantallas táctiles capacitivas permiten interactuar mediante toques y gestos, y son capaces de reproducir video e imágenes de alta resolución. Desde el punto de vista de vigilancia, la pantalla en sí no es una fuente de datos, pero es donde percibimos la información que los sensores captan. A nivel de software, muchas aplicaciones que se abren en pantalla obtienen permisos para registrar clics, desplazamientos y entradas de texto, lo que puede incluir datos sensibles como contraseñas o patrones de uso. Además, tecnologías como *eye-tracking* (rastreo ocular) están en desarrollo para leer la atención del usuario respecto a lo que aparece en la pantalla.

- **Red celular y Wi-Fi**: El teléfono se conecta a Internet principalmente a través de redes móviles (2G, 3G, 4G, 5G) y Wi-Fi. Estos módulos son fundamentales para la comunicación de voz y datos. A través de ellos, cada acción en línea –mensajes, consultas web, transmisiones de aplicaciones– genera tráfico que puede ser interceptado o monitoreado. La comunicación celular involucra protocolos que en teoría están cifrados, pero existen vulnerabilidades conocidas (p. ej. SS7) que permiten a entidades con acceso

a la infraestructura rastrear llamadas, mensajes de texto y ubicación. Las conexiones Wi-Fi también pueden ser espiadas en puntos de acceso inseguros, exponiendo datos sensibles.

- **Biometría (huella dactilar, reconocimiento facial)**: Muchos móviles incorporan sensores biométricos para desbloquear el dispositivo o autenticarse en aplicaciones. La huella dactilar y el reconocimiento facial ofrecen comodidad y un nivel de seguridad mayor que un PIN, porque operan con datos personales únicos. Sin embargo, estos sistemas recopilan y procesan información biométrica que, en caso de ser interceptada o mal gestionada, no es algo que se pueda cambiar (a diferencia de una contraseña). En sistemas abiertos (no propietarios), esta información puede almacenarse de forma local o ser manejada por software que podríamos inspeccionar. Con todo, hay quienes advierten que la biometría puede ser utilizada para vigilancia: empresas o gobiernos podrían exigir acceso al lector de huellas/cámara para verificar identidades o incluso detectar emociones. Mantener la biometría habilitada implica confiar en la política de privacidad del fabricante y desarrollador del software.
- **Cámara y micrófono**: La cámara frontal y trasera son puntos de captura masiva de datos visuales: fotos, videos e incluso escáneres de códigos QR. Estas imágenes pueden revelar nuestra ubicación, nuestras actividades y con quién estamos. El micrófono (normalmente oculto en el cuerpo del teléfono) graba sonido ambiente y voz. Cada vez que una aplicación solicita acceso a la cámara o micrófono, existe el riesgo de que nos graben sin que lo notemos. Incluso sin acceso directo, algoritmos avanzados pueden inferir si estamos escuchando palabras clave (por ejemplo, asistentes virtuales) o guardando audio temporal para activar comandos de voz. Desde la perspectiva de autodefensa electrónica, se recomienda controlar permisos con apps como “Privacy Dashboard” o herramientas de desgooglización, así como cubrir físicamente la cámara cuando no se use y silenciar el micrófono con protectores adecuados.
- **Sensor de proximidad**: Este sensor detecta cuándo el teléfono está cerca del rostro o de un objeto. Su uso típico es apagar automáticamente la pantalla durante una llamada cuando acercamos el móvil a la oreja, evitando toques accidentales. Funciona midiendo la luz infrarroja reflejada. En vigilancia, el sensor de proximidad en sí no es una amenaza directa, pero demuestra que el teléfono conoce cuándo lo acercamos al cuerpo, información que podría combinarse con otros datos para inferir

qué hacemos (por ejemplo, una serie de eventos de cercanía podría sugerir actividad de llamada).

- **Giroscopio y acelerómetro**: Estos sensores miden la orientación y movimiento del dispositivo. El acelerómetro detecta la aceleración lineal en 3 ejes, mientras que el giroscopio mide la rotación angular. Gracias a ellos, el teléfono sabe si lo movemos, lo giramos o lo levantamos para mirarlo, ajustando la interfaz en pantalla (de vertical a horizontal, por ejemplo) o contando pasos (pedometría). Desde la perspectiva del usuario, se usan en juegos, realidad aumentada o para registrar actividad física. Sin embargo, también pueden filtrar información: al analizar las vibraciones y movimientos registrados, algoritmos pueden inferir qué aplicaciones estamos usando (por los patrones de movimiento al tipeo) o incluso reconstruir conversaciones cercanas (a través de vibraciones en la mesa, en experimentos de seguridad informática). En otros casos, estos sensores permiten medir el ruido de la calle o la estabilidad en vehículos (cuando se usa GPS), y compartir esa telemetría. Siempre debemos ser conscientes de que muchas apps solicitan datos de movimiento en segundo plano, por lo que habilitarlos implica ceder información sobre nuestra inercia y posición.
- **Sensor de luz ambiente**: Mide la luminosidad en el entorno cercano al teléfono para ajustar automáticamente el brillo de la pantalla. Esto ahorra batería y protege la vista del usuario. Al ser un sensor pasivo de luz visible, sus lecturas no revelan por sí mismas datos personales. Sin embargo, el patrón de ajuste puede indicar si estamos en exteriores o en interiores, y el teléfono, sabiendo si estamos en un ambiente claro o no, podría inferir nuestro contexto (por ejemplo, encender la pantalla más por la mañana que por la noche). Este sensor no tiene riesgos directos graves, pero pone de manifiesto cómo el teléfono conoce detalles del ambiente físico.
- **Barómetro**: Algunos teléfonos incluyen un barómetro para medir la presión atmosférica. Originalmente concebido para mejorar la precisión en el cálculo de altitud del GPS y monitorear cambios climáticos locales (por ejemplo, ayudar a estimar el piso de un edificio), el barómetro puede en teoría ser usado para conocer la altitud en que se encuentra el usuario. Aunque no revela ubicación horizontal directamente, añade una capa extra de datos sobre la situación del dispositivo. Esto facilita detectar cuántos pisos ha subido alguien y, junto con GPS, puede afinar la posición vertical dentro de una ciudad. De forma maliciosa, combinando presión

con otros datos ambientales (temperatura, altitud de GPS) un atacante podría afinar la localización en mapas, lo que sería relevante en escenarios de vigilancia muy detallada.

- **Termómetro e higrómetro**: Pocos móviles actuales integran sensores de temperatura o humedad ambientales de buena precisión. Sin embargo, algunos dispositivos o accesorios pueden medir la temperatura ambiente o la humedad relativa. Los usos principales incluyen ajuste de rendimiento (evitar sobrecalentamiento) y funciones de bienestar (apps de salud). Los riesgos de privacidad son limitados, pues estos datos meteorológicos son poco sensibles en sí mismos. No obstante, junto con otros sensores de ubicación pueden confirmar el ambiente exacto (por ejemplo, un clima húmedo y caliente podría indicar una región tropical, complementando el GPS).

- **Magnetómetro (Brújula)**: Este sensor mide el campo magnético terrestre, permitiendo al dispositivo conocer la orientación respecto al norte magnético (brújula digital). Es útil para navegación y realidad aumentada. El magnetómetro no recoge datos sobre el usuario, solo la orientación del dispositivo. Sin embargo, requiere calibrarse usando movimientos del teléfono (los típicos 8), registrando patrones adicionales de movimiento. Dado que el campo magnético se ve afectado por objetos metálicos y estructuras, en la práctica el magnetómetro reforzará la capacidad del teléfono para geolocalizarse dentro de un edificio (usando mapas magnéticos interiores), lo que puede enriquecer datos de ubicación.

- **Podómetro**: Es un algoritmo basado en acelerómetro/giroscopio que cuenta pasos y estima distancia recorrida. Sirve en aplicaciones de salud y deportes para cuantificar actividad física. Los datos de podómetro son un ejemplo de datos extremadamente personales: muestran cuándo hacemos ejercicio, cuánto nos desplazamos e incluso podrían indicar cambios de salud o rutina. Por ejemplo, un patrón estable de pasos diarios se puede considerar un fingerprint de la actividad humana. Estos datos suelen enviarse a aplicaciones de salud (propias o de terceros) y si se cruzan con ubicación o registros de actividad podrían revelar muchos detalles sobre el estilo de vida de alguien.

- **Espectrómetro**: Es un sensor muy raro en móviles, presente en algunos modelos especializados. Un espectrómetro mide las propiedades de la luz en diferentes frecuencias (colores) para determinar la composición química de materiales u obtener datos de salud (por ejemplo, medir

frecuencia cardíaca mediante análisis de luz sobre la piel). La inclusión de un espectrómetro convierte al teléfono en un dispositivo de diagnóstico potente: puede, teóricamente, escanear alimentos, detectar minerales o analizar fluidos corporales usando sensores ópticos. Por supuesto, este nivel de supervisión es altamente intrusivo: podría identificarnos por características biométricas (como huella de venas) o revelar qué consumimos. Dada su potencialidad, cualquier espectrómetro debe gestionarse con cautela, pero por ahora su uso es limitado en los dispositivos comunes.

- **IA y aceleradores de cómputo**: No es un sensor en el sentido clásico, pero muchos teléfonos actuales incluyen unidades de procesamiento dedicadas a inteligencia artificial (AI/ML). Estas unidades (a menudo llamadas NPU, unidades de procesamiento neuronal) aceleran tareas como reconocimiento de voz, clasificación de imágenes o predicción de texto. Con ellas se logran funciones avanzadas sin necesidad de enviar datos a la nube. El uso de IA en el dispositivo mejora la privacidad (pues los datos se procesan localmente) y optimiza la batería, pero al mismo tiempo requiere entrenamiento previo con grandes conjuntos de datos. Si el modelo o la app los provee de manera confidencial, el usuario no los ve ni controla fácilmente. Para la autodefensa electrónica, lo relevante es saber qué funciones de IA se activan: por ejemplo, un asistente de voz que analice comandos debe escuchar constantemente el micrófono buscando palabras clave, y aunque el procesamiento sea local, podría almacenar fragmentos de audio. Por esto, es prudente revisar y limitar las funciones de IA que no sean estrictamente necesarias.

- **NFC (Near Field Communication)**: Es un módulo de corto alcance que permite comunicación inalámbrica bidireccional a distancias muy cortas (unos pocos centímetros). Se utiliza en pagos móviles (digitando tarjetas de crédito sin contacto), emparejamiento rápido de dispositivos y lecturas de etiquetas RFID. NFC transmite datos de la cuenta o credenciales de forma cifrada, pero requiere proximidad física al lector. Desde el punto de vista de seguridad, es bastante fiable por su corto alcance: un tercero no puede interceptar fácilmente la señal sin estar a centímetros de nosotros. Sin embargo, un atacante muy cercano podría interferir. En general, el principal riesgo de NFC es más sobre aplicaciones maliciosas que aprovechan permisos NFC para realizar pagos no autorizados (por ello, se requiere confirmación del usuario). En términos de vigilancia, NFC no expone información a larga distancia, pero forma parte del ecosistema

global de seguimiento si sus datos (como transacciones de pago) se agregan a perfiles más amplios.

- **GPS (Sistema de Posicionamiento Global)**: Es uno de los componentes más conocidos: mediante satélites y otras redes (a veces asistido por torres de celular o Wi-Fi) calcula la posición geográfica del dispositivo con alta precisión. El GPS permite funciones de navegación en tiempo real, geolocalización de fotografías, seguimiento deportivo, entre otras. Al mismo tiempo, cada activación del GPS genera un registro de ubicación exacto. Si las aplicaciones obtienen permiso para usarlo, podrían registrar continuamente dónde estamos y a qué hora. Estos datos son extremadamente sensibles, pues establecen patrones de vida: trabajo, hogar, lugares de visita, ritmos diarios. El GPS se desactiva manualmente con frecuencia en pro de la privacidad; sin embargo, existen técnicas de triangulación a través de torres celulares o Wi-Fi que pueden ubicarnos incluso con el GPS apagado. Para mayor control, es recomendable usar sistemas de localización lo más mínimamente posible (por ejemplo, configurar la ubicación en “Solo mientras se usa la app” o usar GPS solo con apps de total confianza).
- **LIDAR / Sensor de profundidad**: Algunos teléfonos avanzados incluyen sensores de tiempo de vuelo o LIDAR (Light Detection And Ranging) que emiten pulsos de luz para medir distancias con precisión y crear mapas de profundidad. Esto se emplea en aplicaciones de realidad aumentada (para colocar objetos virtuales en el entorno) y cámaras para enfocar mejor o crear efectos de retrato. El LIDAR no capta información “personal” visible, pero sí un mapa 3D del espacio cercano. Con lecturas de LIDAR se pueden reconstruir ambientes interiores y, en teoría, identificar a las personas cercanas por su contorno. Actualmente su uso principal es fotográfico, pero en términos de vigilancia podría complementar el seguimiento de movimiento (por ejemplo, determinar cuántas personas hay en una habitación).

En resumen, nuestros teléfonos reúnen una miríada de sensores y funciones de conectividad que nos ofrecen comodidades insospechadas –como guiar una ruta a pie o permitir un pago contactless– pero también constituyen canales de información continua. Cada módulo puede ser una fuente de datos sensible. Entender el funcionamiento interno del dispositivo nos ayuda a ser conscientes de los riesgos: por ejemplo, evitar dejar habilitado el Bluetooth o GPS permanentemente, revisar periódicamente los permisos de las aplicaciones, y

considerar alternativas más seguras cuando sea posible. En las siguientes secciones veremos cómo estos datos pueden ser aprovechados por entidades externas y qué estrategias existen para protegernos.

2. Modelos y aparatos de vigilancia

La vigilancia electrónica sobre los teléfonos móviles opera en varios niveles: desde los dispositivos mismos hasta la infraestructura de red y las empresas que acumulan datos. En esta sección se describen primero las **amenazas directas en las redes telefónicas**, que son los métodos técnicos para interceptar o manipular comunicaciones móviles. Luego se aborda la **telemetría y perfilamiento**: la recopilación masiva de datos de los usuarios para trazar perfiles detallados de comportamiento.

2.1 Amenazas de seguridad en redes telefónicas

- **Stingrays (IMSI Catchers)**: Son dispositivos de intercepción que actúan como torres de telefonía móvil falsas. Un Stingray hace creer a los teléfonos cercanos que es la antena celular más poderosa y cercana, logrando que los móviles se conecten a él en lugar de a las antenas legítimas. De esta forma, el Stingray captura el identificador único del teléfono (IMSI) y puede espiar llamadas, mensajes y datos sin que el usuario lo note. El uso de Stingrays suele asociarse a fuerzas de seguridad y agencias estatales (por ejemplo, la policía los usa para localizar a sospechosos). Sin embargo, también pueden emplearse ilegalmente o por entidades privadas sin autorización. El peligro radica en que un Stingray puede derribar la encriptación regular de las comunicaciones celulares y forzar la conexión en canales menos seguros. Además de espiar datos, puede ubicar la posición de varios teléfonos simultáneamente dentro de la zona de cobertura falsa.

- **SIM jacker**: Se refiere a ataques que buscan controlar o extraer información del chip SIM del teléfono. Un método común es enviar un SMS malicioso que explota vulnerabilidades en la tarjeta SIM para ejecutar código sin consentimiento (esto ocurrió con vulnerabilidades conocidas llamadas “Simjacker”). Mediante este ataque, un SMS aparentemente inocuo puede forzar al teléfono a responder con su localización o iniciar llamadas y mensajes. Dado que el código malicioso se ejecuta directamente en la tarjeta SIM, las aplicaciones del sistema no detectan la intrusión fácilmente. El SIM jacker permite a atacantes remotos rastrear la ubicación del dispositivo a través de la red móvil sin que el usuario lo perciba, e incluso escuchar el entorno mediante la activación encubierta del altavoz.

La mitigación requiere actualizaciones de seguridad en las tarjetas SIM, cosa que muchos usuarios no verifican por su cuenta.

- **SIM swapping (robo de SIM)**: Es un fraude que consiste en clonar o transferir el número de teléfono a una tarjeta SIM en poder del atacante. En la práctica, el delincuente convence al proveedor de telefonía (o lo piratea) para que le asigne el número telefónico de la víctima a un SIM propio. Así, la víctima pierde el servicio y no recibe llamadas o mensajes entrantes, mientras el atacante recibe las comunicaciones dirigidas a ese número. Esto permite al atacante interceptar códigos de verificación de SMS (que protegen muchas cuentas en línea) y eludir la autenticación en dos pasos, accediendo potencialmente a cuentas bancarias o de redes sociales. El SIM swapping es peligroso porque permite un control total del canal de voz/SMS. Para protegernos, es recomendable usar autenticadores de aplicaciones en lugar de SMS, y exigir al proveedor medidas de seguridad adicionales (PIN de la cuenta, preguntas de seguridad).

- **Ataques SS7/SIGTRAN**: El protocolo SS7 es el conjunto de estándares que rige la señalización de redes móviles convencionales (2G/3G/4G). Originalmente, SS7 no fue diseñado con fuertes medidas de seguridad, ya que se basó en la confianza entre operadoras. Sin embargo, esta confianza es ahora un problema: atacantes sofisticados han demostrado que se puede explotar SS7 para rastrear números de teléfono globalmente, redirigir llamadas, leer mensajes SMS o clonar la localización en tiempo real. SIGTRAN es una versión de SS7 sobre IP. Debido a estas vulnerabilidades históricas, gobiernos y hackers con acceso a la infraestructura de telecomunicaciones pueden monitorear tráfico móvil a gran escala. En la práctica, esto significa que incluso con la encriptación entre el teléfono y la torre, los metadatos (quién llama a quién, cuándo y desde dónde) pueden interceptarse. Los usuarios no tienen forma directa de impedir la explotación de SS7, salvo exigir a los proveedores y legisladores que refuercen la seguridad de la red.

- **Cell Tower Dump**: Consiste en capturar la información emitida por una torre celular a todos los teléfonos que están dentro de su alcance. Cada torre transmite periódicamente datos públicos que incluyen las identificaciones de los teléfonos conectados (como el IMEI y la IMSI). Un atacante puede simplemente llevar un dispositivo especializado cerca de una torre y registrar todas estas transmisiones pasivas, obteniendo una lista de todos los móviles en la zona, sus identificadores únicos y

frecuencias de aparición. Con esta técnica no es necesario instalar nada en los teléfonos; la torre misma delata a los usuarios. Luego, combinando estos datos con otras fuentes (por ejemplo, registros de llamadas o ubicación), es posible monitorear movimientos y crear bases de datos masivas de ubicaciones históricas. Dado que este método es relativamente sencillo técnicamente, representa una amenaza real para la privacidad en entornos densamente poblados: no solo a individuos con rastreo activo, sino cualquier persona que pase por allí y sea capturada en un barrido.

En conjunto, estas amenazas demuestran que las redes celulares son vulnerables en múltiples frentes. Para la soberanía digital, es vital adoptar prácticas de defensa: cifrar las conversaciones (por ejemplo con aplicaciones de mensajería seguras en lugar de llamadas convencionales), emplear VPN cuando usemos datos móviles, deshabilitar la señal celular cuando no la necesitemos, y estar alerta ante actividades sospechosas (llamadas perdidas extrañas, cambio repentino a otra torre). Aunque no podemos controlar la infraestructura, sí podemos reducir el tiempo de exposición y la información que compartimos con la red.

2.2 Telemetría y perfilamiento

Aun sin ataques directos, las redes y las aplicaciones recopilan por defecto datos de **telemetría**: información sobre el comportamiento del teléfono y el usuario. Cada mensaje enviado, cada localización registrada y cada interacción con el dispositivo genera metadatos (datos sobre los datos) que pueden cruzarse para obtener perfiles detallados. Esto se ve con especial intensidad en el modelo de **capitalismo de vigilancia**, en el que empresas tecnológicas (y también gobiernos) obtienen beneficios económicos o estratégicos a partir de la vigilancia masiva.

- **Patrones de comportamiento humano**: La telemetría incluye registros de llamadas (cuánto hablamos y con quién), uso de aplicaciones (qué apps usamos, por cuánto tiempo), historial de navegación (búsquedas y sitios visitados) y ubicación GPS o de torres. Al agregar meses o años de estos datos, es posible inferir hábitos: rutina diaria, preferencias en entretenimiento, estado de salud (por los apps de ejercicio o sueño), relaciones sociales e incluso creencias políticas (por la información buscada). Por ejemplo, visitas frecuentes a un centro médico en horarios específicos podría indicar una enfermedad crónica; llamar repetidamente a ciertos números revela redes de contacto; comprobar la hora de últimas interacciones puede detectar cambios de comportamiento (como

insomnio). Los algoritmos de perfilamiento intentan convertir esta gigantesca base de información en “insights” comprensibles: “público adulto interesado en deportes”, “grupo de trabajo en la empresa X”, etc. Cada usuario es transformado en un conjunto de características que pueden ser vendidas a anunciantes o a quien pague por ese perfil.

- **Capitalismo de vigilancia**: Este concepto, acuñado por analistas críticos, describe el sistema económico donde los datos personales se convierten en activos lucrativos. A cambio de servicios aparentemente gratuitos (redes sociales, correo electrónico, apps) los proveedores recopilan nuestras estadísticas de uso. Cada clic, pulso o likes alimenta algoritmos de recomendación y de venta de publicidad. La plataforma centraliza información e incluso las intenciones de compra. En la práctica, esto significa que nuestra relación con el teléfono está mediada por entidades que vigilan nuestra actividad para diseñar campañas publicitarias personalizadas (incluso antes de que sepamos que necesitamos algo). Con ello se condiciona la autonomía: nuestras preferencias y decisiones de consumo acaban previstas o guiadas por lo que el perfil sugiere de nosotros. En un plano más profundo, puede generar sesgos sociales (por ejemplo, en qué tipo de noticias se nos muestran) y decisiones automatizadas (créditos, seguros, empleo) basadas en nuestra telemetría. Ser conscientes de esto refuerza la idea de que mantener el control sobre nuestros datos es esencial para preservar la libertad individual.

- **Device fingerprints (huellas digitales)**: Aparte de la telemetría normal, muchas plataformas obtienen un **fingerprint** del dispositivo. Este fingerprint combina datos únicos del hardware y el software: modelo de teléfono, resolución de pantalla, versión de sistema, identificadores de navegador, lista de fuentes instaladas, características de la tarjeta gráfica, etc. Con esto crean un “pasaporte” digital que identifica nuestro dispositivo a pesar de las medidas clásicas de privacidad (como borrar cookies o usar una VPN). Al navegar por sitios web o abrir apps que recopilan esta información, el servidor puede reconocer de vuelta al teléfono aunque cambiemos de dirección IP. El fingerprinting permite que nos rastreen pasivamente a través de múltiples servicios sin alertarnos. Por ejemplo, usar una app de noticias y luego el navegador de internet puede vincularse al mismo dispositivo mediante su fingerprint. En términos de autodefensa, los fingerprints representan un reto, ya que es difícil evitarlos sin renunciar a muchos servicios. Sin embargo, ciertos sistemas operativos alternativos buscan minimizar la uniformidad de los teléfonos (es decir,

reducir la predictibilidad de las huellas digitales) y así dificultar el rastreo uniforme.

- **Metadatos**: Además de unirse en perfiles, los metadatos individuales (por ejemplo, ubicación geográfica, registros de hora, duración de llamadas, remitentes de mensajes) se almacenan en bases de datos de operadoras, redes sociales y aplicaciones. Aunque un metadato aislado parezca inofensivo, cruzando millones de ellos surgen patrones reveladores. Por ejemplo, un metadato de ubicación a mediodía cada día en un edificio específico revela nuestro lugar de trabajo; otro conjunto a determinadas horas en una zona residencial señala nuestro hogar. Los metadatos también incluyen nuestras interacciones con publicidad y publicaciones en redes sociales (tipo de contenido que curtimos o compartimos). Combinados con IA, incluso la agrupación de metadatos puede predecir estados de ánimo o predisposiciones del usuario. El peor riesgo es que estos datos pueden usarse sin el consentimiento explícito del usuario: por ejemplo, empresas que analizan “big data” pueden decidir cerrar un seguro o aumentar tasas basándose en patrones extraídos de metadatos. Para resistir este modelo, además de elegir servicios con políticas de privacidad más estrictas, es crucial ejercer nuestros derechos cuando existan (solicitar borrado de datos, limitar el seguimiento en la medida de lo posible).

- **Cruzamiento de datos**: Una de las prácticas más sofisticadas es combinar información de distintas fuentes. Pensemos: una compañía de telecomunicaciones conoce a qué horas nos conectamos a la red y a qué sitios web accedemos; una red social conoce con quién hablamos y qué vemos en Internet; una app de mapas sabe por dónde transitamos; una tienda en línea conoce nuestras compras. Solas, estas bases son valiosas; juntas, son casi omniscientes. El **data matching** o cruzamiento permite que se relacione un identificador único (por ejemplo, nuestro número de teléfono o una dirección de correo) con todos estos servicios. Por ejemplo, muchos móviles están vinculados a una cuenta de Google o Apple que se utiliza en varios contextos. Al cruzar los logs de esa cuenta con la red celular y las interacciones en aplicaciones, se obtiene un perfil multidimensional: amistades, actividades, preferencias, estado de salud potencial, nivel socioeconómico, creencias políticas… Esta información cruzada puede ser vendida a publicistas, o utilizada por estados para vigilancia masiva. Desde la perspectiva de la autodefensa digital, comprender el poder del cruzamiento insta a minimizar los puntos de

enlace: usar servicios independientes (no basados en Google/Apple), reducir enlaces directos entre aplicaciones (por ejemplo, no iniciar sesión con la misma cuenta en todos lados) y desconfiar de permisos que compartan datos entre apps.

En su conjunto, la telemetría y el perfilamiento muestran una realidad: casi cualquier cosa que hacemos con el móvil es susceptible de ser registrada, analizada y monetizada. La **soberanía digital** requiere reconocer estos modelos de vigilancia encubierta. Solo así podemos valorar alternativas y prácticas más seguras: optar por software de código abierto, cifrar las comunicaciones, apoyarnos en comunidades que respetan la privacidad, y sobre todo, educar a los usuarios sobre los impactos de cada configuración.

3. Teléfonos y sistemas alternativos – Sistemas libres, cómodos y seguros

Frente al dominio de los sistemas operativos móviles convencionales (principalmente Android y iOS), existe un ecosistema creciente de **sistemas operativos alternativos y dispositivos** orientados a la privacidad, la seguridad y la autonomía del usuario. A continuación se describen los más destacados, sus ventajas y desventajas, con comparativas generales entre ellos. Todos comparten el objetivo de minimizar el rastreo por parte de grandes corporaciones, pero difieren en enfoque, madurez y compatibilidad.

- **LineageOS**: Es una distribución de Android de código abierto, creada como sucesora de CyanogenMod. LineageOS ofrece una experiencia similar a Android “puro” pero sin las capas propietarias añadidas por fabricantes o Google. Soporta cientos de modelos diferentes de teléfonos, actualizándolos incluso cuando el fabricante original deja de dar soporte. Entre sus ventajas destacan la frecuencia de actualizaciones de seguridad y la ausencia de software preinstalado de terceros. El usuario mantiene el control total: es posible habilitar o deshabilitar cada aplicación del sistema, revisar el código fuente y no requiere cuenta alguna con Google para funcionar. Sin embargo, al carecer de Google Play Services por defecto, muchas aplicaciones populares pueden no funcionar correctamente a menos que se instale una alternativa (como microG). Además, la instalación de LineageOS requiere desbloquear el bootloader y flashear el dispositivo, un proceso que puede resultar complicado para usuarios novatos. En términos de seguridad, LineageOS es notablemente mejor que

Android estándar, aunque depende de la limpieza del proyecto: dado que es comunitario, la rapidez de parches depende de los voluntarios.

- **GrapheneOS**: Este es un sistema Android muy endurecido, diseñado principalmente para dispositivos Pixel de Google (en especial, modelos recientes). Su foco es la privacidad y seguridad extrema: desactiva muchos servicios que corren en segundo plano, endurece los mecanismos de cifrado y minimiza los posibles puntos de ataque del sistema. GrapheneOS no permite instalar Google Play Services ni ninguna otra fuente cerrada de forma oficial. Esto significa que el usuario es completamente libre de instalar solo aplicaciones de fuentes confiables (F-Droid, Aurora, etc.), evitando código propietario. Las ventajas son enormes en seguridad: por ejemplo, GrapheneOS tiene un modo "Sandboxed Play" opcional para ejecutar apps con los servicios de Google dentro de un contenedor muy restringido. Sin embargo, el sistema es mucho más restrictivo para el usuario medio: la disponibilidad de apps es menor (se depende de apps de código abierto o portadas manualmente), y al limitar funciones puede romper la compatibilidad con servicios modernos que requieren Google. Además, solo funciona en unos pocos dispositivos Pixel, con actualizaciones específicas para ellos. Por lo tanto, es ideal para usuarios avanzados que priorizan la seguridad por encima de la comodidad.

- **Maemo Leste**: Basado en Linux (la rama Maemo), es un sistema operativo libre para móviles inspirado en la experiencia de los antiguos Nokia con Maemo/Harmattan (p. ej., el Nokia N900). Maemo Leste es una distribución de Linux completa adaptada a pantallas táctiles. Ofrece un entorno tipo escritorio a la vez que apps móviles, enfocándose en privacidade a través de software abierto. Puede ejecutarse en algunos dispositivos legacy (sobre todo Nokia) y en hardware de Pine64. Aunque su comunidad es pequeña y el catálogo de aplicaciones limitado, permite una libertad total (se instala software directamente desde repositorios de Linux, con soporte de apps Debian y personalizaciones). Sus ventajas son la apertura total (al igual que las distros de Linux para PC) y la posibilidad de auditar completamente el sistema. Su inconveniente principal es la compatibilidad de hardware y software: muchos componentes del teléfono pueden no estar soportados (como cámaras o acelerómetros) debido a la falta de controladores libres, y muchas aplicaciones populares no están disponibles o no corren fácilmente sobre Maemo Leste.

- **Ubuntu Touch**: Desarrollado por UBports (heredero del proyecto original de Canonical), Ubuntu Touch es la versión móvil de Ubuntu Linux. Se caracteriza por su interfaz convergente: se acerca a una experiencia de escritorio cuando se conecta a monitor. En móviles, proporciona aplicaciones basadas en tecnologías web y contenedores. Sus beneficios incluyen un modelo de aplicaciones centrado en la privacidad (cada app vive en un contenedor aislado y se definen explícitamente los permisos). Ubuntu Touch corre en diversos modelos de teléfonos (especialmente algunos Nexus, OnePlus y Pixel adaptados). Comparado con Lineage, Ubuntu Touch es más revolucionario en interfaz, pero su ecosistema de aplicaciones es relativamente pequeño. Ofrece una experiencia Unix pura en móvil, lo que lo hace atractivo para usuarios avanzados. Sin embargo, la compatibilidad de hardware puede ser problemática: algunas funciones (como mensajería SMS o ciertas cámaras) pueden no estar plenamente soportadas en todos los dispositivos. Por eso, Ubuntu Touch es ideal para quienes valoran un sistema realmente libre y adaptado por la comunidad, sabiendo que podrían sacrificar algunos aspectos de usabilidad.
- **PinePhone**: No es un sistema sino un **hardware de móvil** libre, diseñado por la empresa Pine64 para correr sistemas Linux de código abierto. Viene desbloqueado (bootloader libre) y con switches físicos para desconectar Wi-Fi, Bluetooth, cámara o micrófono, reforzando la privacidad. El PinePhone se vende en distintas ediciones (uno con hardware más básico para ahorro y otro "Pro" con mayor potencia). Funciona con múltiples sistemas operativos Linux móviles (como Mobian, postmarketOS, Plasma Mobile, Ubuntu Touch). Su punto fuerte es la versatilidad: puedes instalar varias distribuciones y experimentar. Sin embargo, como teléfono primario tiene limitaciones: su rendimiento es modesto comparado con móviles comerciales, la cámara es básica y su autonomía corta. Aun así, el PinePhone ejemplifica la filosofía "libre" en móviles: tú controlas todo el software, puedes compilar el kernel, y no hay bloqueo por parte de fabricantes. Su comunidad es entusiasta, con continuas mejoras de software. Para quienes buscan soberanía total, es un excelente dispositivo de entrada, siempre que no dependan de una experiencia pulida de "smartphone tradicional".
- **Murena Phone** (/e/ OS): Se comercializa como un móvil "privacidad" con un fork de Android conocido como /e/ OS (eFoundation). Murena vende teléfonos y tablets con este sistema preinstalado. /e/ OS es básicamente Android libre de Google, reemplazando los servicios de Google por

alternativas propias (por ejemplo, en lugar de Google Play Services se usa microG). Además integran servicios en la nube (correo, calendario, nube de archivos) que prometen no rastrear datos. Las ventajas de Murena son la facilidad de uso (tiene app store gráfico con acceso a muchas apps Android) y soporte directo del fabricante (incluyen actualizaciones OTA). Comparado con GrapheneOS, es mucho más amigable para el usuario promedio. Sin embargo, su enfoque es menos extremo en privacidad: aunque eliminan Google, usan servicios centralizados de eFoundation, los cuales, aunque son de código abierto, aún almacenan datos del usuario (en su nube). Además, los teléfonos Murena son hardware re-etiquetado de marcas existentes; no están tan enfocados en la seguridad a nivel de hardware. Son adecuados para quienes quieren un Android "sin Google" listo para usar, sacrificando algunas garantías de seguridad máximas.

- **Plasma Mobile**: Proyecto liderado por KDE para portar el entorno gráfico Plasma (conocido en Linux de escritorio) a móviles. Plasma Mobile corre en Linux móviles como Mobian o postmarketOS. Está diseñado para interfaces táctiles y ofrece un ambiente moderno. Lo interesante es la integración con otros proyectos KDE (por ej. aplicaciones integradas como navegador, correo, etc.) y su enfoque en ser modular. No depende de Android para nada; es un stack Linux puro. Esto significa un altísimo nivel de auditabilidad y privacidad (al provenir de proyectos del software libre con millones de usuarios en PC). Sin embargo, como Ubuntu Touch, su ecosistema móvil aún es limitado. Plasma Mobile suele exhibirse en dispositivos como el PinePhone o el Librem 5. Las ventajas incluyen su estética pulida y la filosofía GNU/Linux; las desventajas son que algunas funciones del teléfono no siempre funcionan perfectamente (módulos de radio, cámara) debido a la juventud del proyecto.

- **TizenOS**: Es un sistema operativo basado en Linux, desarrollado principalmente por Samsung (y la Fundación Linux). Se usa en teléfonos Samsung antiguos y en otros dispositivos (TVs, wearables, electrodomésticos). Tizen está menos abierto que las demás opciones en esta lista: es de código abierto en algunos componentes, pero gran parte del desarrollo está controlado por Samsung. Como sistema alternativo, Tizen es curioso: ofrece un entorno independiente de Android (por ejemplo, los teléfonos Z3 con Firefox OS usados Tizen para ciertas funciones de bajo costo). Su filosofía es más corporativa; no está orientado al usuario preocupado por la privacidad. Dicho esto, al ser menos popular que Android, no está tan perfilado para apps de terceros, lo que reduce en

parte el ecosistema. No es exactamente una opción popular para usuarios de soberanía, pero se incluye por ser un intento de diversificar el mercado.

- **Droidian**: Es otro proyecto que lleva Debian GNU/Linux a teléfonos. Mantiene la base sólida de Debian, ofreciendo acceso a miles de paquetes de software libre. Droidian funciona junto con el entorno de Plasma Mobile en algunos dispositivos (por ejemplo, variantes del PinePhone). La ventaja es que cualquier software de Debian podría compilarse para móvil (incluyendo herramientas de privacidad o servidores locales). Similar a Mobian (otro nombre de Debian en móvil), Droidian prioriza la libertad de software. La desventaja es típica de las portaciones: hardware limitado y poca pulcritud, pensada más para entusiastas que para uso diario.

- **KaiOS**: KaiOS merece mención aunque es muy diferente: es un sistema para teléfonos “feature phones” que habilita muchas funciones de smartphone en dispositivos básicos. Se basa en un fork de Firefox OS (HTML5) y se ejecuta en móviles de bajo costo (Nokia 8110, JioPhone). Ofrece acceso a apps (WhatsApp, YouTube, etc.) en una interfaz simple no táctil. Desde la perspectiva de soberanía, KaiOS es mixto: por un lado, democratiza el acceso digital en poblaciones sin smartphones, pero por otro, tiene componentes propietarios y es respaldado por una empresa (KaiOS Technologies). Adicionalmente, KaiOS puede incluir Google servicios (dependiendo del socio fabricante). No es una plataforma orientada a privacidad, pero representa una categoría de móvil alternativo.

- **PostmarketOS**: Proyecto que busca llevar una distribución de Linux ligera y duradera a dispositivos móviles viejos. El objetivo de PostmarketOS es permitir que smartphones de otras épocas (a veces obsoletos) puedan revivir ejecutando Linux nativo. Se enfoca en eficiencia energética y en proporcionar un sistema modular, soportando varios entornos gráficos (Plasma Mobile, Sxmo, etc.). PostmarketOS destaca por su optimización: promete que un teléfono de cinco años puede mantenerse vivo con actualizaciones de software por otros cinco. Al igual que Mobian, ofrece una experiencia libertaria y sin Google. Los pros son el uso de software estable y mantenido, así como la longevidad de los equipos. El contra es que el soporte completo de hardware depende de la comunidad, y no todos los componentes (cámara, sensores) quedan funcionales en los dispositivos.

- **SailfishOS**: Desarrollado por la empresa finlandesa Jolla, es un sistema operativo basado en el kernel de Linux pero con un stack de middleware propietario (aunque están comprometidos con el código abierto). Sailfish

tiene su propio sistema de UI, distinto a Android. Su ventaja principal es la capacidad de ejecutar aplicaciones de Android (mediante una capa de compatibilidad), lo cual facilita el acceso a muchas apps conocidas mientras se usa un SO diferente. Jolla ha hecho énfasis en la privacidad y en no depender de Google; sin embargo, al tener componentes cerrados en el middleware, la auditabilidad total es limitada. Está orientado a usuarios empresariales y entusiastas. Ha existido en varios dispositivos Jolla y en algunos PinePhone. Ofrece una experiencia pulida y gestos intuitivos, pero su ecosistema de apps nativas sigue siendo pequeño, y se ha visto superado por el crecimiento de otros proyectos más libres.

- **Librem Phone (Purism Librem 5)**: Purism es una compañía centrada en seguridad y privacidad. El Librem 5 es un teléfono de hardware abierto pensado para correr PureOS (derivado de Debian) con un enfoque extremo en seguridad: tiene interruptores físicos para desactivar la cámara, micrófono, Wi-Fi, Bluetooth y la antena celular. El sistema operativo elimina todo rastro de servicios de Google y cifra por defecto. El Librem Phone es posiblemente el más “sólido” en términos de garantías de hardware libre y privacidad, pero también es un teléfono de nicho: su rendimiento y cámara no están al nivel de buques insignia de otras marcas, y su precio es elevado. Además, Purism controla qué software se incluye en el sistema, y el enfoque es más empresarial. Aun así, es ejemplar como dispositivo autodefensa: cualquier usuario que quiera un teléfono hecho exclusivamente para soberanía electrónica consideraría un Librem 5.

- **MobianOS**: Es simplemente la distribución oficial de Debian para móviles, a menudo corrigiendo aspectos que PostmarketOS no cubre. Funciona en PinePhone y otros dispositivos. Ofrece el escritorio móvil de GNOME adaptado a pantallas pequeñas, o bien Plasma. Mobian es libre, estable y recibe actualizaciones de seguridad rápidamente gracias al respaldo de Debian. Al ser más sencillo de instalar (instalar Debian estándar en móvil con algunas modificaciones) es menos experimental que PostmarketOS, pero maneja la misma idea de libre completo. La compatibilidad de aplicaciones es rica (al usar repos de Debian), pero la experiencia de usuario puede ser menos amigable para lo cotidiano.

- **Volla Phone**: Es un teléfono comercializado en Alemania por la empresa Volla con dos opciones de sistema: Volla OS (basado en Android Open Source Project, sin servicios de Google) o Ubuntu Touch. El hardware es

genérico (fabricado por diversos partners chinos) y el sistema Volla OS incluye el launcher Graphene X para proteger la privacidad. Volla se centra en mercados de Europa como alternativa privada a Android de Google. Ofrece una experiencia “lista para usar” para quienes desean salir de Google pero sin perder el ecosistema Android completo. Las actualizaciones de seguridad no son tan frecuentes como en Lineage o Graphene, pero el paquete es cómodo para el usuario común.

En la comparación general, podemos resumir: sistemas como **GrapheneOS** y **Librem 5** sacrifican la comodidad para obtener máxima seguridad, restringiendo el ecosistema y el hardware soportado. En cambio, proyectos como **LineageOS**, **Murena** o **Volla OS** buscan un término medio: mayor libertad que Android convencional, pero manteniendo compatibilidad con la mayoría de aplicaciones y hardware. Los sistemas basados en **Linux puro** (Maemo Leste, Ubuntu Touch, Plasma Mobile, PostmarketOS, Mobian) apuntan a quienes valoran el software libre y no necesitan todas las apps comerciales. **KaiOS** y **TizenOS** son más casos especiales: el primero democratiza acceso digital en móviles muy básicos, y el segundo es más bien un sistema corporativo cerrado que raramente se asocia a la autodefensa del usuario.

Entre estos, las comunidades de desarrollo son clave. LineageOS tiene un enorme respaldo global con desarrolladores en todo el mundo, garantizando un amplio soporte de dispositivos y actualizaciones. GrapheneOS cuenta con un equipo pequeño pero altamente especializado, centrado en seguridad. Ubuntu Touch, PinePhone/Mobian, Plasma Mobile y PostmarketOS también tienen comunidades vibrantes aunque más reducidas, que comparten entre sí hardware (por ejemplo, todos apoyan al PinePhone). En términos de **seguridad y privacidad**, los que parten de Android sin Google (Lineage con microG, Murena, Volla) son un paso significativo adelante, mientras que los basados en Linux completo elevan aún más la soberanía al eliminar por completo el código no libre. Para cada usuario, la elección dependerá de sus prioridades: facilidad de uso, disponibilidad de apps o nivel de control absoluto. Lo importante es que hoy en día ya existen múltiples alternativas robustas a los sistemas dominantes, lo cual es en sí mismo un indicio positivo hacia mayor autonomía digital.

4. Tiendas de aplicaciones alternativas a Play Store – Tiendas libres y seguras

El ecosistema de aplicaciones es otro ámbito crítico. Google Play Store y Apple App Store dominan la distribución de software móvil, pero incluyen restricciones

y mecanismos de seguimiento. Existen **tiendas de apps alternativas** que ofrecen catálogos de aplicaciones libres y verificación comunitaria. A continuación se analizan las más conocidas y se comparan con Play Store.

- **F-Droid**: Es la tienda de apps libres más reconocida para Android. Funciona como repositorio de aplicaciones de código abierto; cada app en F-Droid debe tener su código fuente disponible y licencia libre. En lugar de un servidor centralizado de Google, F-Droid es mantenido por voluntarios; la instalación típica se hace descargando su APK desde su web oficial (para teléfonos sin Play Store). Entre sus ventajas destacan que las apps solo contienen libreta de direcciones donde se detalla qué características contienen (lo cual permite revisiones de seguridad públicas) y que no hay seguimiento de usuarios (no requiere crear cuenta ni enviar información personal). Además, F-Droid detecta y avisa si las apps consumen recursos inusuales (por ejemplo, piden acceso innecesario a ubicación). Su catálogo es más pequeño que el de Google Play, ya que excluye apps propietarias. Incluye aplicaciones muy comunes en el software libre (como Signal, Telegram, navegadores libres, utilidades, etc.). Para quien ya usa un sistema Android “desgooglizado” o con microG, F-Droid es la principal fuente de aplicaciones seguras. La filosofía de F-Droid es purista: todo tiene que ser libre. Un inconveniente es que las actualizaciones dependen de mantenedores voluntarios, por lo que a veces pueden ser más lentas que en Play.

- **Zapstore**: Es un proyecto más reciente que también busca proveer un repositorio de aplicaciones open source. Se puede considerar similar a F-Droid en su filosofía de transparencia, pero pretende ampliar el catálogo incluyendo aplicaciones de terceros, siempre y cuando el código esté disponible o el APK se pueda verificar. Zapstore enfatiza en la fácil instalación de la tienda misma, con un proceso de autoupdate que recoge apps populares (según su comunidad). Al ser un proyecto incipiente, su catálogo es todavía limitado, pero crece gradualmente. Su punto fuerte es la búsqueda centrada en privacidad y la interconexión con redes libres. Presenta la información de las apps en un formato claro, indicando licencias y repositorios de código. En comparación con Play Store, Zapstore no integra pago ni cuentas de usuario (aunque es posible que en el futuro soporte métodos de donación a desarrolladores), por lo que elimina la tendencia de rastreo con ID personales. Su seguridad proviene de la transparencia: cualquiera puede auditar el código de Zapstore y las apps que almacena.

- **Accrescent**: Es otra tienda alternativa dedicada a Android. Está alojada en GitHub y su objetivo es facilitar el acceso a aplicaciones sin Google Play. Su nombre proviene de “acrescentar” (añadir). Accrescent pretende ser una especie de biblioteca de apps sin trackers, verificadas y distribuidas directamente. Al igual que F-Droid, exige que el código de las apps sea libre y verificado. Su diferencia es que se promociona como una plataforma de la comunidad para recopilar apps útiles, con un enfoque en seguridad. Aunque no es tan conocida, puede complementarse con F-Droid: por ejemplo, si no encuentras una app en F-Droid, podrías buscarla en Accrescent. El sistema de validación de Accrescent incluye comprobaciones de integridad de las apps para asegurarse de que no hayan sido alteradas maliciosamente. Al carecer de una empresa detrás, la tienda depende de colaboradores para expandir la biblioteca de software.
- **Obtainium**: Es un proyecto de tienda de aplicaciones construido sobre la API de Google Play pero sin Google, desarrollado por la comunidad de microG. Permite descargar APKs directamente desde los repositorios de Google Play en formato libre, sin necesidad de una cuenta Google. Está diseñado para complementar a F-Droid: por ejemplo, si una app libre no está en F-Droid, se puede conseguir su APK en Obtainium sin instalar la Play Store. Como ventaja, su catálogo incluye básicamente cualquier app disponible en Play Store (siempre que el desarrollador del APK lo permita). Las descargas se hacen a través de la API de Play, pero no se comunican datos del usuario a Google porque no se requiere credencial. Es una opción útil para obtener aplicaciones cerradas que no se encuentran de otra forma (aunque esto va en contra del ideal de apps libres). En términos de seguridad, Obtainium confía en la propia validación de Google (ya que baja directamente de esa fuente) y en que el usuario eventualmente compruebe si la app es confiable. Su filosofía es pragmática: “Obtain what you need”, sin añadir trackers propios. Aunque aún está en desarrollo, ofrece un puente para quienes abandonan Play pero aún quieren aplicaciones populares.

Comparativa con Google Play Store

Google Play Store es la tienda oficial de Android y, si bien tiene un catálogo inmenso, está atada a Google Play Services y a una cuenta Google. Play Store implementa sus propias políticas de revisión y detección de apps maliciosas (como Play Protect), pero ha sido cuestionada por incluir apps con trackers intrusivos o por censurar aplicaciones fuera de su ecosistema. Además, Play Store

rastrea automáticamente qué descargamos, cuándo actualizamos, y usa estos datos para recomendar contenido o para perfiles de usuario. Las tiendas alternativas (F-Droid, Zapstore, etc.) no dependen de una cuenta centralizada ni comparten información personal con terceros. A cambio, suelen ofrecer menos aplicaciones y carecen de sistemas automáticos de monetización (por ejemplo, integrados en-app purchases).

En cuanto a **seguridad y verificación**, Play Store realiza un análisis inicial a las apps (a menudo detectando malware) y lanza actualizaciones automáticas. Sin embargo, ha habido casos de apps maliciosas que pasaron sus filtros. F-Droid y similares revisan manualmente cada app, enfocándose más en el código abierto y en detectar conductas sospechosas a través de inspección. El usuario de tiendas libres debe ser más proactivo: instalar solo lo necesario, preferir apps auditadas, y revisar permisos.

En resumen, las tiendas alternativas enfatizan la **filosofía del software libre**: control del usuario sobre su software y transparencia. No persiguen maximizar ganancias, sino ofrecer una opción ética y segura. Al migrar a estas tiendas, se abandona la comodidad de Play Store (apps de pago centralizadas, actualizaciones automáticas universales, reseñas masivas, etc.) pero se gana en privacidad y autonomía. Además, fomentan la existencia de desarrolladores que publiquen libremente sin depender de intermediarios. Para la autodefensa electrónica, usar F-Droid (o Zapstore, etc.) significa usar software cuyo funcionamiento se puede inspeccionar y que no incorpora rastreadores ocultos, alineándose así con una estrategia más soberana.

5. Herramientas para desgooglear el teléfono

“Desgooglizar” un móvil se refiere a eliminar o reemplazar los servicios propietarios de Google (o de otros grandes proveedores) que monitorean nuestra actividad. En Android, Google Play Services es el núcleo que da acceso a funcionalidades de geolocalización, notificaciones push, sincronización de cuentas, etc. Sustituirlo implica algunos pasos técnicos y el uso de herramientas especiales. A continuación se describen **Shizuku, Canta y Aurora Store**, tres herramientas clave para este proceso, así como el flujo general para lograr un teléfono más libre.

- **Shizuku**: Es una aplicación que facilita que otras apps utilicen APIs de Android con privilegios de sistema sin requerir acceso de root permanente. Shizuku opera en segundo plano como un servicio que corre con permisos elevados (iniciándose por adb o temporalmente). Gracias a él, es posible

que utilidades de ajuste o de personalización (como cambiar permisos, modificar configuraciones avanzadas, o habilitar funciones bloqueadas) lo hagan sin root. En el contexto de desgoogleizar, Shizuku se usa a menudo en conjunción con apps que necesitan permisos especiales (por ejemplo, para instalar certificaciones del sistema, usar microG o controlar datos en background). La ventaja de Shizuku es que reduce la necesidad de rootear el teléfono completo, lo cual preserva cierta integridad del sistema. Para el usuario avanzado, Shizuku brinda más libertad, pero se usa principalmente para auditoría o modificaciones profundas que de otro modo requerirían desbloquearlo.

- **Canta**: Este es un proyecto específico, usualmente una herramienta o guía automatizada desarrollada por la comunidad, cuyo objetivo es instalar microG y herramientas asociadas en un dispositivo Android. MicroG es una implementación de código abierto de los servicios de Google Play; permite que apps que dependen de Google (p. ej. para notificaciones push o autenticación con cuenta Google) funcionen sin tener el software propietario instalado. **Canta** (en algunos casos llamado “script Canta”) automatiza la configuración de microG, Magisk (si se usa root), y otros ajustes para reemplazar los servicios de Google. Su nombre sugiere “cantar” o guiar al teléfono hacia la libertad. Utilizar Canta implica seguir un proceso que puede requerir habilitar opciones de desarrollador, instalar un paquete de microG (a menudo vía Magisk), y configurar cuentas de Google si se desea hacer login sin los servicios oficiales. Las ventajas de Canta son que simplifica un proceso complicado; las desventajas son que no siempre es compatible con todos los dispositivos o versiones de Android, y al ser un proyecto de terceros, se asume que confías en el desarrollador del script (sin embargo, al ser de código abierto puedes revisar lo que hace).

- **Aurora Store**: Es quizás la herramienta más conocida para usuarios que quieren un reemplazo de la tienda Google Play en Android libre. Aurora Store es un cliente de código abierto que permite descargar e instalar aplicaciones de la Play Store sin tener la aplicación oficial ni una cuenta Google. Opera conectándose a la API de Google Play usando credenciales anónimas (o propias si el usuario las tiene). Con Aurora es posible buscar cualquier app del catálogo de Google, visualizar sus descripciones y actualizar las instalaciones. A nivel de seguridad, Aurora no comparte datos de cuenta (usa una “cuenta fantasma” por defecto) y no incluye rastreadores adicionales. Su gran ventaja es que abre el acceso al vasto

repertorio de apps Android cerradas cuando no existen alternativas libres, todo sin dejar el teléfono en estado “Google dependiente”. Sin embargo, hay riesgo: dado que algunas apps descargadas requieren los servicios de Google (por ejemplo, apps bancarias o juegos con DRM), algunas funciones pueden no funcionar o necesitar un “módulo de compatibilidad” adicional.

Proceso de desgoogleización paso a paso

1. **Copia de seguridad**: Antes de cualquier modificación, hay que hacer backup de datos importantes (fotos, contactos, mensajes). Esto puede implicar usar herramientas locales (por ejemplo, exportar contactos a un archivo) o apps de copia de seguridad offline. Se recomienda evitar respaldos en la nube de Google en este paso.

2. **Desinstalar o deshabilitar servicios de Google**: En algunos casos, simplemente desactivar las apps de Google desde Configuración (o con ADB) es suficiente. En otros, es mejor flashear un sistema limpio (como LineageOS o GrapheneOS). Si se opta por flashear un nuevo sistema operativo sin Google, el teléfono queda “de fábrica” limpio de Google.

3. **Instalar microG**: Si queremos seguir usando apps Android que dependen de Google (WhatsApp, GMaps, etc.), se debe instalar microG, que simula las APIs necesarias. Esto puede implicar root o usar un sistema como Aurora/Haystack. Shizuku/Canta suelen facilitar este paso. Con microG, podemos conectar nuestra cuenta de Google al nivel de notificaciones y autenticación, sin tener Google Play Services reales.

4. **Elegir tiendas alternativas**: Tras eliminar Play Store, debemos establecer otras fuentes. Lo normal es instalar F-Droid primero. Luego, si necesitamos aplicaciones adicionales, se instala Aurora Store (desde F-Droid o directamente). También se puede incorporar Zapstore o Accrescent desde sus APKs. Con esto, recuperamos la capacidad de descargar aplicaciones seguras.

5. **Administrar permisos y configuraciones**: Usar herramientas de control de permisos (como en Ajustes de privacidad del sistema o apps específicas) para revisar qué aplicaciones tienen acceso a cámara, micrófono, ubicación, etc. Es recomendable otorgar los mínimos permisos necesarios y revisar periódicamente si las apps siguen requiriendo esos permisos. Shizuku también puede ayudar a revisar y ajustar estos permisos a nivel de sistema.

6. **Restaurar datos y configuración manualmente**: En la medida de lo posible, restaurar la información sin depender de Google. Por ejemplo, reconfigurar cuentas de correo en cliente de correo independiente, importar contactos desde archivos, migrar chats de mensajería usando exportaciones (como WhatsApp exportando chats con una opción nativa), o usar herramientas de recuperación local.

7. **Alternativas a servicios populares**: Considerar reemplazar ciertos servicios de Google por alternativas libres: usar OpenStreetMap en lugar de Google Maps, Signal en lugar de Hangouts, Nextcloud en lugar de Google Drive, etc. Cada sustitución reduce la dependencia de la infraestructura de Google.

8. **Mantener el sistema actualizado por otros medios**: Al no usar Google Play, las actualizaciones automáticas cambian. Hay que actualizar manualmente a través de F-Droid (para apps libres), y para el sistema, confiar en las actualizaciones OTA proporcionadas por LineageOS, GrapheneOS u otro SO alternativo. Es vital revisar periódicamente las actualizaciones de seguridad.

Beneficios y riesgos

Beneficios de desgoogleizar: mejora sustancial de la privacidad (Google deja de rastrearnos), prolongación de la vida útil del dispositivo (con sistemas alternativos que actualizan más allá del soporte oficial) y fortalecimiento de la autodefensa digital (controlamos qué software corre en el teléfono). También fomenta la autoeducación tecnológica: al entender mejor cómo funciona Android y sus dependencias, el usuario toma decisiones más informadas.

Riesgos y desafíos: Inicialmente puede ser complejo y requiere conocimientos técnicos. Algunos servicios o aplicaciones comunes dejarán de funcionar (por ejemplo, pagos móviles con Google Pay no serán posibles sin Google), y habrá que pasar por inconvenientes ocasionales (apps que dicen “No se puede descargar en tu dispositivo” o que rechazan ejecución sin Play Services). Además, al depender de herramientas de terceros (Aurora, Shizuku, microG), se introduce un nivel de confianza en esos proyectos comunitarios (aunque suelen ser transparentes). Existe también el riesgo de configuraciones incorrectas: si se instala una app maliciosa de una tienda no verificada, se pierde seguridad. En general, la transición exige paciencia y, sobre todo, un compromiso de aprendizaje.

En resumen, las herramientas mencionadas (Shizuku, Canta, Aurora Store) ofrecen caminos para liberarse de Google gradualmente. No hay una única "fórmula mágica": cada usuario puede adaptar los pasos a sus necesidades, eligiendo un equilibrio entre funcionalidad y privacidad. Lo esencial es entender que hay opciones para controlar nuestro propio teléfono, y que cada pequeño cambio (desde desactivar un permiso hasta instalar microG) contribuye a un móvil más soberano.

6. Conclusiones

A lo largo de esta guía se ha analizado en profundidad el papel que juegan los teléfonos móviles en la era digital y cómo podemos tomar el control sobre ellos para proteger nuestra soberanía electrónica. Los smartphones actuales son máquinas complejas, repletas de sensores y conexiones que, al mismo tiempo que nos brindan numerosas facilidades, pueden ser canales de explotación de nuestra privacidad. Entender su funcionamiento interno (pantallas, cámaras, redes, giroscopios, etc.) y nuestras propias dinámicas de uso (donde la adicción a la atención es el motor económico) nos ayuda a darnos cuenta de la magnitud de los datos que generamos.

Las amenazas no provienen solo de hackers individuales, sino de sistemas estructurados: desde interceptores de red (Stingrays, SS7) hasta modelos comerciales que recolectan metadatos para perfilarnos. Ante estos riesgos, la soberanía digital cobra sentido como un enfoque estratégico: debemos concebir el teléfono como un territorio personal que requiere defensas. Para ello, hemos visto diversas **herramientas** y **estrategias**: elegir sistemas operativos alternativos (como LineageOS, GrapheneOS, Linux móviles) que no envíen datos a servidores centrales, emplear tiendas de aplicaciones libres (F-Droid, Zapstore, etc.) en lugar de plataformas comerciales cerradas, y utilizar utilidades que remuevan o reemplacen componentes propietarios (como microG mediante Canta o acceder a apps con Aurora Store). Cada una de estas acciones tiene un impacto: por ejemplo, al usar LineageOS y F-Droid, reducimos notablemente la exposición a rastreadores invisibles y dependemos menos de Amazon/Google/Apple.

Es importante remarcar que la autodefensa electrónica no es un estado absoluto sino un proceso. Incluso con los cambios técnicos, debemos mantener un comportamiento crítico: actualizar el software regularmente, revisar permisos de aplicaciones, y educar a otros usuarios sobre prácticas seguras. La adopción de estas medidas suele venir acompañada de la creación de comunidades de apoyo: foros, chats o grupos dedicados al software libre en móviles donde se comparten

guías y soluciones. En el largo plazo, la suma de estos esfuerzos puede empoderar a los usuarios y presionar a la industria: cuanta más gente utilice sistemas libres o tiendas alternativas, más fuerza tendrá el argumento de la privacidad como derecho.

Finalmente, la perspectiva de **soberanía digital** nos invita a ver más allá del teléfono como un dispositivo aislado. Se trata de entender nuestra relación con la tecnología en su conjunto: qué datos queremos entregar, a quién se los damos y con qué propósito. Los teléfonos móviles son una parte crítica de este panorama, pero los principios aquí expuestos –control del software, minimización de la captura de datos, uso de herramientas libres– pueden extrapolarse a otros ámbitos (computadoras, redes sociales, servicios en la nube).

En conclusión, la resistencia y la autodefensa electrónica con teléfonos móviles se fundamenta en el conocimiento y la acción: conocer cómo funcionan y cómo se vulneran los dispositivos, y tomar decisiones tecnológicas coherentes (como usar sistemas operativos alternativos y tiendas libres). Recomendamos a los lectores empezar por pequeños pasos: protegerse contra las amenazas más evidentes (usar cifrado de mensajes, desactivar servicios innecesarios) e ir incorporando progresivamente cambios mayores (como migrar a sistemas abiertos o instalar microG). La soberanía digital no es solo responsabilidad de un experto: cada usuario consciente puede contribuir a construir un entorno digital más libre y seguro.

7. Apéndices

- **Recursos adicionales**: Existe una vasta documentación en línea sobre cada sistema y herramienta mencionada. Las comunidades de cada proyecto suelen mantener wikis y foros (por ejemplo, la wiki de LineageOS o los foros de Pine64) donde se explican pasos de instalación y solución de problemas. Igualmente, en plataformas de desarrollo como GitHub se encuentran los repositorios oficiales de Aurora Store, Shizuku, Canta y otros. Por razones de autonomía del informe no se incluyen hipervínculos, pero se recomienda buscar los nombres oficiales de cada proyecto para acceder a sus recursos.
- **Guías rápidas de instalación**: A modo de resumen, a continuación se describen a grandes rasgos cómo abordar algunas instalaciones:
- ***Instalar LineageOS***: desbloquear el gestor de arranque del móvil mediante el comando `fastboot oem unlock`, descargar la imagen oficial de LineageOS y flashearla con `fastboot flash`, luego instalar el paquete de

aplicaciones opcionales (GApps) o microG según preferencia. Cada dispositivo tiene pasos específicos disponibles en la documentación oficial.

- ***Configurar microG con Canta***: normalmente implica activar la opción de instalación desde fuentes desconocidas, instalar el script de Canta (por ejemplo, desde F-Droid si está disponible) y ejecutarlo, lo que automatiza la descarga e instalación de microG Services Core, droidguard dummy y configures el acceso a notificaciones.
- ***Instalar Aurora Store***: descargar el APK desde F-Droid o su sitio de GitHub, otorgar permisos necesarios y al iniciar elegir entre conectar una cuenta Google anónima o usar credenciales propias (opcional). Luego se puede buscar apps y descargarlas igual que en Play Store.
- **Conceptos clave**: A manera de recordatorio, algunos conceptos técnicos relevantes:
- ***Root***: modo avanzado de Android que da acceso total al sistema (alternativa a Shizuku para ciertos ajustes).
- ***Bootloader***: software que arranca el sistema; debe desbloquearse para flashear un nuevo SO.
- ***Permisos***: autorizaciones que da el usuario a cada app (se pueden gestionar en Ajustes o con apps especializadas).
- **Herramientas de respaldo**: Antes de modificar el teléfono, se pueden usar programas como `adb backup` (para Android) o utilidades de copia en PC, asegurando los datos personales y las configuraciones de las apps.
- **Comunidades de apoyo**: Se sugiere participar en comunidades como foros de XDA Developers (para desarrollo Android), Reddit (subreddits de privacidad y de cada proyecto), y grupos de Telegram/Matrix dedicados a privacidad digital. Allí se pueden resolver dudas específicas y recibir ayuda de otros usuarios experimentados.

Este informe busca servir como base técnica y práctica para que cualquier persona interesada pueda avanzar hacia una mayor soberanía con su teléfono móvil. En futuras entregas (Parte 2, 3, etc.), se podrán abordar temas más avanzados o específicos, pero por ahora nos enfocamos en establecer los fundamentos necesarios para la resistencia y autodefensa electrónica desde el dispositivo móvil.